EXACT EXPONENT OF REMAINDER TERM OF GELFOND'S DIGIT THEOREM IN BINARY CASE

VLADIMIR SHEVELEV

Abstract. We give a simple formula for the exact exponent in the remainder term of Gelfond's digit theorem in the binary case.

1. Introduction

Denote for integer $m > 1$, $a \in [0, m-1]$.

$$T^{(j)}_{m,a}(x) = \sum_{0 \le n < x,\ \ n \equiv a \mod m,\ \ s(n) \equiv j \mod 2} 1, \qquad j = 1, 2 \tag{1}$$

where $s(n)$ is the number of 1's in the binary expansion of n.

A. O. Gelfond [5] proved that

$$T^{(j)}_{m,a}(x) = \frac{x}{2m} + O(x^{\lambda}), \qquad j = 0, 1, \tag{2}$$

where

$$\lambda = \frac{\ln 3}{\ln 4} = 0.79248125\ldots \tag{3}$$

Recently, the author proved [9] that the exponent λ in the remainder term in (2) is the best possible when m is a multiple of 3 and is not the best possible otherwise.

In this paper we give a simple formula for the exact exponent in the remainder term of (2) for an arbitrary m. Our method is based on constructing a recursion relation for the Newman-like sum corresponding to (1)

$$S_{m,a}(x) = \sum_{0 \le n < x,\ n \equiv a \mod m} (-1)^{s(n)}, \tag{4}$$

1991 *Mathematics Subject Classification.* 11A63.

It is sufficient for our purposes to deal with odd numbers m . Indeed, it is easy to see that, if m is even, then

$$S_{m,a}(2x) = (-1)^a S_{\frac{m}{2},\lfloor\frac{a}{2}\rfloor}(x). \tag{5}$$

For an odd $m > 1$, consider the number $r = r(m)$ of distinct cyclotomic cosets of 2 modulo m [6, pp.104-105]. E.g., $r(15) = 4$ since for $m = 15$ we have the following 4 cyclotomic cosets of 2: $\{1, 2, 4, 8\}, \{3, 6, 12, 9\}, \{5, 10\}$, $\{7, 14, 13, 11\}$.

Note that, if $C_1, \ldots, C_r$ are all different cyclotomic cosets of 2 $\mod m$, then

$$\bigcup_{j=1}^{r} C_j = \{1, 2, \ldots, m-1\}, \qquad C_{j_1} \cap C_{j_2} = \varnothing, \ \ j_1 \neq j_2. \tag{6}$$

Let h be the least common multiple of $|C_1|, \ldots, |C_r|$:

$$h = [|C_1|, \ldots, |C_r|] \tag{7}$$

Note that h is of order 2 modulo m. (This follows easily, e.g., from Exercise 3, p. 104 in [8]).

Definition 1. *The exact exponent in the remainder term in (2) is* $\alpha = \alpha(m)$ *if*

$$T^j_{m,a}(x) = \frac{x}{2m} + O(x^{\alpha+\varepsilon}),$$

and

$$T^j_{m,a}(x) = \frac{x}{2m} + \Omega(x^{\alpha-\varepsilon}), \qquad \forall \varepsilon > 0.$$

Our main result is the following.

Theorem 1. *If* $m \geq 3$ *is odd, then the exact exponent in the remainder term in (2) is*

$$\alpha = \max_{1\leq l\leq m-1} \left(1 + \frac{1}{h \ln 2} \sum_{k=0}^{h-1} \left(\ln \left|\sin \frac{\pi l 2^k}{m}\right|\right)\right) \tag{8}$$

Note that, if 2 is a primitive root of an odd prime p, then $r = 1, \ h = p-1$. As a corollary of Theorem 1 we obtain the following result.

Theorem 2. *If p is an odd prime, for which 2 is a primitive root, then the exact exponent in the remainder term in (2) is*

$$\alpha = \frac{\ln p}{(p-1)\ln 2}. \tag{9}$$

Theorem 2 generalizes the well-known result for $p = 3$ ([7], [2], [1]). Furthermore, we say that 2 is a *semiprimitive root* modulo p if 2 is of order $\frac{p-1}{2}$ modulo p and the congruence $2^x \equiv -1 \mod p$ is not solvable. E.g., 2 is of order $8 \mod 17$, but the congruence $2^x \equiv -1 \mod 17$ has the solution $x = 4$. Therefore, 2 is not a semiprimitive root of 17. The first primes for which 2 is a semiprimitive root are (see[10], A 139035)

$$7, 23, 47, 71, 79, 103, 167, 191, 199, 239, 263, \dots \tag{10}$$

For these primes we have $r = 2$, $h = \frac{p-1}{2}$. As a second corollary of Theorem 1 we obtain the following result.

Theorem 3. *If p is an odd prime for which 2 is a semiprimitive root, then the exact exponent α in the remainder term in (2) is also given by (9).*

In Section 2 we provide an explicit formula for $S_{m,a}(x)$, while in Sections 3-5 we prove Theorems 1-3.

2. Explicit formula for $S_{m,a}(x)$

Let $\lfloor x \rfloor = N$. We have

$$S_{m,a}(N) = \sum_{n=0, m|n-a}^{N-1} (-1)^{s(n)} = \frac{1}{m} \sum_{t=0}^{m-1} \sum_{n=0}^{N-1} (-1)^{s(n)} e^{2\pi i \frac{(n-a)t}{m}}$$

$$= \frac{1}{m} \sum_{t=0}^{m-1} \sum_{n=0}^{N-1} e^{2\pi i (\frac{t}{m}(n-a) + \frac{1}{2} s(n))}. \tag{11}$$

Note that the interior sum is of the form

$$\Phi_{a,\beta}(N) = \sum_{n=0}^{N-1} e^{2\pi i (\beta(n-a) + \frac{1}{2} s(n))}, \qquad 0 \le \beta < 1. \tag{12}$$

Putting

$$F_\beta(N) = e^{2\pi i \beta a} \Phi_{a,\beta}(N), \tag{13}$$

we note that $F_\beta(N)$ does not depend on a.

Lemma 1. *If* $N = 2^{\nu_0} + 2^{\nu_1} + \ldots + 2^{\nu_\sigma}$, $\nu_0 > \nu_r > \ldots > \nu_\sigma \geq 0$, *then*

$$F_\beta(N) = \sum_{g=0}^{\sigma} e^{2\pi i(\beta \sum_{j=0}^{g-1} 2^{\nu_j} + \frac{g}{2})} \prod_{k=0}^{\nu_g - 1} (1 + e^{2\pi i(\beta 2^k + \frac{1}{2})}). \tag{14}$$

Proof. Let $\sigma = 0$. Then by (12) and (13)

$$F_\beta(N) = \sum_{n=0}^{N-1} (-1)^{s(n)} e^{2\pi i \beta n}$$

$$= 1 - \sum_{j=0}^{\nu_0 - 1} e^{2\pi i \beta 2^j} + \sum_{0 \leq j_1 < j_2 \leq \nu_0 - 1} e^{2\pi i \beta (2^{j_1} + 2^{j_2})} - \ldots \tag{15}$$

$$= \prod_{k=0}^{\nu_0 - 1} (1 - e^{2\pi i \beta 2^k}),$$

which corresponds to (14) for $\sigma = 0$.

Assuming that (14) is valid for every N with $s(N) = \sigma + 1$, let us consider $N_1 = 2^{\nu_\sigma} b + 2^{\nu_{\sigma+1}}$ where b is odd, $s(b) = \sigma + 1$ and $\nu_{\sigma+1} < \nu_\sigma$. Let

$$N = 2^{\nu_\sigma} b = 2^{\nu_0} + \ldots + 2^{\nu_\sigma}; \quad N_1 = 2^{\nu_0} + \ldots + 2^{\nu_\sigma} + 2^{\nu_{\sigma+1}}.$$

Notice that for $n \in [0, \nu_{\sigma+1})$ we have

$$s(N + n) = s(N) + s(n).$$

Therefore,

$$F_\beta(N_1) = F_\beta(N) + \sum_{n=N}^{N_1 - 1} e^{2\pi i(\beta n + \frac{1}{2} s(n))}$$

$$= F_\beta(N) + \sum_{n=0}^{\nu_{\sigma+1} - 1} e^{2\pi i(\beta n + \beta N + \frac{1}{2}(s(N) + s(n)))}$$

$$= F_\beta(N) + e^{2\pi i(\beta N + \frac{1}{2} s(N))} \sum_{n=0}^{\nu_{\sigma+1} - 1} e^{2\pi i(\beta n + \frac{1}{2} s(n))}.$$

Thus, by (14) and (15),

$$F_\beta(N_1) =$$

$$\sum_{g=0}^{\sigma} e^{2\pi i(\beta \sum_{j=0}^{g-1} 2^{\nu_j} + \frac{g}{2})} \prod_{k=0}^{\nu_g - 1} (1 + e^{2\pi i(\beta 2^k + \frac{1}{2})}$$

$$+ e^{2\pi i(\beta \sum_{j=0}^{\sigma} 2^{\nu_j} + \frac{\sigma+1}{2})} \prod_{k=0}^{\nu_{g+1}-1} \left(1 + e^{2\pi i(\beta 2^k + \frac{1}{2})}\right)$$

$$= \sum_{g=0}^{\sigma+1} e^{2\pi i(\beta \sum_{j=0}^{g-1} 2^{\nu_j} + \frac{g}{2})} \prod_{k-0}^{\nu_g - 1} \left(1 + e^{2\pi i(\beta 2^k + \frac{1}{2})}\right). \blacksquare$$

Formulas (11)-(14) give an explicit expression for $S_m(N)$ as a linear combination of products of the form

$$\prod_{k=0}^{\nu_g - 1} \left(1 + e^{2\pi i(\beta 2^k + \frac{1}{2})}\right), \quad \beta = \frac{t}{m}, \quad 0 \le t \le m-1. \tag{16}$$

Remark 1. *One may derive (14) from a very complicated general formula of Gelfond* [5]*. However, we prefered to give an independent proof.*

In particular, if $N = 2^\nu$, then from (11)-(13) and (15) for

$$\beta = \frac{t}{m}, \quad t = 0, 1, \ldots, m-1, \tag{17}$$

we obtain the known formula cf. [3]:

$$S_{m,a}(2^\nu) = \frac{1}{m} \sum_{t=1}^{m-1} e^{-2\pi i \frac{t}{m} a} \prod_{k=0}^{\nu-1} (1 - e^{2\pi i \frac{t}{m} 2^k}). \tag{18}$$

3. Proof of Theorem 1

Consider the equation of order r

$$z^r + c_1 z^{r-1} + \ldots + c_r = 0 \tag{19}$$

with the roots

$$z_j = \prod_{t \in C_j} \left(1 - e^{2\pi i \frac{t}{m}}\right), \quad j = 1, 2, \ldots, r. \tag{20}$$

Notice that for $t \in C_j$ we have

$$\prod_{k=n+1}^{n+h}\left(1-e^{2\pi i\frac{t2^k}{m}}\right)=\left(\prod_{t\in C_j}\left(1-e^{2\pi i\frac{t}{m}}\right)\right)^{\frac{h}{h_j}}=z_j^{\frac{h}{h_j}}, \tag{21}$$

where h is defined by (7). Therefore, for every $t \in \{1,\dots,m-1\}$, according to (19) we have

$$\prod_{k=n+1}^{n+rh}\left(1-e^{2\pi i\frac{t2^k}{m}}\right) + c_1\prod_{k=n+1}^{n+(r-1)h}\left(1-e^{2\pi i\frac{t2^k}{m}}\right)+\cdots + c_{r-1}\prod_{k=n+1}^{n+h}\left(1-e^{2\pi i\frac{t2^k}{m}}\right)+c_r=0. \tag{22}$$

After multiplication by $e^{-2\pi i\frac{t}{m}a}\prod_{k=0}^{n}\left(1-e^{2\pi i\frac{t2^k}{m}}\right)$ and summing over $t = 1,2,\dots,m-1$, by (18) we find

$$S_{m,a}\left(2^{n+rh+1}\right)+c_1S_{m,a}\left(2^{n+(r-1)h+1}\right)+\cdots+c_{r-1}S_{m,a}\left(2^{n+h+1}\right)+c_rS_{m,a}\left(2^{n+1}\right)=0. \tag{23}$$

Moreover, using the general formulas (11)-(14) for a positive integer u, we obtain the equality

$$S_{m,a}\left(2^{rh+1}u\right)+c_1S_{m,a}\left(2^{(r-1)h+1}u\right)+\cdots+c_{r-1}S_{m,a}\left(2^{h+1}u\right)+c_rS_{m,a}(2u)=0. \tag{24}$$

Putting here

$$S_{m,a}(2^u)=f_{m,a}(u), \tag{25}$$

we have

$$f_{m,a}(y+rh+1)+c_1f_{m,a}(y+(r-1)h+1)+\cdots+c_{r-1}f_{m,a}(y+h+1)+c_rf_{m,a}(y+1)=0, \tag{26}$$

where

$$y = \log_2 u. \tag{27}$$

The characteristic equation of (27) is

$$v^{rh} + c_1 v^{(r-1)h} + \cdots + c_{r-1} v^h + c_r = 0. \tag{28}$$

A comparison of (28) and (20)-(21) shows that the roots of (28) are

$$v_{j,w} = e^{\frac{2\pi i w}{h}} \prod_{t \in C_j} \left(1 - e^{2\pi i \frac{t}{m}}\right)^{\frac{1}{h}}, \quad w = 0, \ldots, h-1, \ j = 1, 2, \ldots, r. \tag{29}$$

Thus,

$$v = \max |v_{j,l}| = 2 \max_{1 \le l \le m-1} \left(\prod_{k=0}^{h-1} \left| \sin \frac{\pi l 2^k}{m} \right| \right)^{\frac{1}{h}}. \tag{30}$$

Generally speaking, some numbers in (20) could be equal. In view of (29), the $v_{j,w}$'s have the same multiplicities. If η is the maximal multiplicity, then according to (27), (30)

$$S_{m,a}(u) = f_{m,a}(\log_2 u) = O\left((\log_2 u)^{\eta - 1} u^{\frac{\ln v}{\ln 2}} \right). \tag{31}$$

Nevertheless, at least

$$S_{m,a}(u) = \Omega\left(u^{\frac{\ln v}{\ln 2}} \right). \tag{32}$$

Indeed, let, say, $v = |v_{1,w}|$ and in the solution of (27) with some natural initial conditions, all coefficients of $y^{j_1} v_{1,w}^y, \ \ j_1 \le \eta - 1, \ \ w = 0, \ldots, h-1,$ are 0. Then $f_{m,a}(y)$ satisfies a difference equation with the characteristic equation not having roots $v_{1,w}$ and the corresponding relation for

$S_{m,a}(2^n)$ (see (23)) has the characteristic equation (20) without the root z_1. This is impossible since by (18) and (21) we have

$$S_{m,a}(2^{h+1}) = \frac{1}{m} \sum_{j=1}^{r} \sum_{t \in C_j} e^{-2\pi i \frac{t}{m} a} \prod_{k=1}^{h} (1 - e^{2\pi i \frac{t}{m} 2^k}) = \frac{1}{m} \sum_{j=1}^{r} \sum_{t \in C_j} e^{-2\pi i \frac{t}{m} a} z_j^{\frac{h}{h_j}}.$$

Therefore, not all considered coefficients vanish, and (32) follows. Now from (30)- (32) we obtain (8).■

Remark 2. *In (8) it is sufficient to let l run over a system of distinct representatives of the cyclotomic cosets $C_1, \ldots, C_r$ of 2 modulo m.*

Remark 3. *It is easy to see that there exists $l \geq 1$ such that $|C_l| = 2$ if and only if m is a multiple of 3. Moreover, in the capacity of l we can take $\frac{m}{3}$. Now from (8) choosing $l = \frac{m}{3}$ we obtain that $\alpha = \lambda = \frac{\ln 3}{\ln 4}$. This result was obtained in* [9] *together with estimates of the constants in $S_{m,0}(x) = O(x^\lambda)$ and $S_{m,0}(x) = \Omega(x^\lambda)$ which are based on the proved in* [9] *formula*

$$S_{m,0}(x) = \frac{3}{m} S_{3,0}(x) + O(x^{\lambda_1})$$

for $\lambda_1 = \lambda_1(m) < \lambda$ and Coquet's theorem [2].

Example 1. *Let $m = 17,\ a = 0$. Then $r = 2,\ h = 8$,*

$$C_1 = \{1, 2, 4, 8, 16, 15, 13, 9\}, \ \ C_2 = \{3, 6, 12, 7, 14, 11, 5, 10\}.$$

The calculation of $\alpha_l = 1 + \frac{1}{8 \ln 2} \sum_{k=0}^{17} (\ln |\sin \frac{\pi l 2^k}{17}|)$ for $l = 1$ and $l = 3$ gives

$\alpha_1 = -0.12228749\ldots,\quad \alpha_3 = 0.63322035\ldots$. *Therefore by Theorem 1, $\alpha = 0.63322035\ldots$. Moreover, we are able to prove that*

$$\alpha = \frac{\ln(17 + 4\sqrt{17})}{\ln 256}.$$

Indeed, according to (23), for $n = 0$ and $n = 1$ we obtain the system $(S_{17,0} = S_{17})$:

$$\begin{cases} c_1 S_{17}(2^9) + c_2 S_{17}(2) = -S_{17}(2^{17}) \\ c_1 S_{17}(2^10) + c_2 S_{17}(2^2) = -S_{17}(2^{18}) \end{cases} \tag{33}$$

By direct calculations we find

$$S_{17}(2) = 1, \ \ S_{17}(2^2) = 1, \ \ S_{17}(2^9) = 21,$$
$$S_{17}(2^{10}) = 29, \ \ S_{17}(2^{17}) = 697, \quad S_{17}(2^{18}) = 969.$$

Solving (33) we obtain

$$c_1 = -34, \quad c_2 = 17.$$

Thus, by (23) and (24)

$$S_{17}(2^{n+17}) = 34S_{17}(2^{n+9}) - 17S_{17}(2^{n+1}), \quad n \geq 0, \tag{34}$$

$$S_{17}(2^{17}x) = 34S_{17}(2^{9}x) - 17S_{17}(2x), \quad x \in \mathbb{N}. \tag{35}$$

Putting furthermore

$$S_{17}(2^{x}) = f(x), \tag{36}$$

we have

$$f(y+17) = 34f(y+9) - 17(y+1),$$

where $y = \log_2 x$. Hence,

$$f(x) = O\left((17+4\sqrt{17})^{\frac{x}{8}}\right),$$

$$S_{17}(x) = O\left((17+4\sqrt{17})^{\frac{1}{8}\log_2 x}\right) = O(x^{\alpha}), \tag{37}$$

where

$$\alpha = \frac{\ln(17+4\sqrt{17})}{\ln 256} = 0.633220353\ldots$$

4. Proofs of Theorems 2 and 3

a) By the conditions of Theorem 2 we have $r = 1, \;\; h = p-1$. Using (8) we have

$$\alpha = 1 + \frac{1}{(p-1)\ln 2}\ln\prod_{k=0}^{p-2}\left|\sin\frac{\pi 2^k}{p}\right| = 1 + \frac{1}{(p-1)\ln 2}\ln\prod_{l=1}^{p-1}\sin\frac{\pi l}{p}.$$

Furthermore, using the identity [4, p.378],

$$\prod_{l=1}^{p-1}\sin\frac{l\pi}{p} = \frac{p}{2^{p-1}}$$

we find

$$\alpha = 1 + \frac{1}{(p-1)\ln 2}\left(\ln p - (p-1)\ln 2\right) = \frac{\ln p}{(p-1)\ln 2}. \blacksquare$$

Remark 4. *In this case, (24) has the simple form*

$$S_{p,a}(2^p u) + c_1 S_{p,a}(2u) = 0.$$

Since in the case of $a = 0$ or 1 we have

$$S_{p,a}(2) = (-1)^{s(a)},$$

while in the case of $a \geq 2$,

$$S_{p,a}(2a) = (-1)^{s(a)},$$

then putting

$$u = \begin{cases} 1, & a = 0, 1, \\ a, & a \geq 2, \end{cases}$$

we find

$$c_1 = (-1)^{s(a)+1} \begin{cases} S_{p,a}(2^p), & a = 0, 1, \\ S_{p,a}(a2^p), & a \geq 2 \end{cases} .$$

In particular, if $p = 3,\ a = 2$ we have $c_1 = S_{3,2}(16) = -3$ and

$$S_{3,2}(8u) = 3S_{3,2}(2u).$$

Remark 5. *If Artin's conjecture on the infinity of primes for which 2 is a primitive root is true, then for $\alpha = \alpha(p)$ we have*

$$\liminf_{p \to \infty} \alpha(p) = 0.$$

b) By the conditions of Theorem 3 we have $r = 2, \quad h = \frac{p-1}{2}$, such that for cyclotomic cosets of 2 modulo p

$$C_1 = -C_2.$$

Therefore, in (8) for $l_1 = 1$ and $l_2 = p - 1$ we obtain the same values. Thus,

$$\alpha = 1 + \frac{2}{(p-1)\ln 2} \ln \left(\prod_{l=1}^{p-1} \sin \frac{\pi l}{p} \right)^{\frac{1}{2}} = \frac{\ln p}{(p-1)\ln 2}. \blacksquare$$

Using Theorems 1-3, in particular we find

$$\alpha(3) = 0.7924..., \alpha(5) = 0.5804..., \alpha(7) = 0.4678..., \alpha(11) = 0.3459,$$

$$\alpha(13) = 0.3083..., \alpha(17) = 0.6332..., \alpha(19) = 0.2359..., \alpha(23) = 0.2056...,$$

$$\alpha(29) = 0.1734..., \alpha(31) = 0.6358..., \alpha(37) = 0.1447..., \alpha(41) = 0.4339...,$$

$$\alpha(43) = 0.6337..., \alpha(47) = 0.1207...$$

.

References

[1] J.-P. Allouche and J. Shallit. *Automatic Sequences: Theory, Applications, Generalizations*, Cambridge University Press, 2003.

[2] J. Coquet, A summation formula related to the binary digits, *Invent. Math.* **73** (1983),107-115.

[3] M. Drmota and M. Skalba, Rarified sums of the Thue-Morse sequence, *Trans. AMS* **352,**no.2 (1999), 609-642.

[4] G. Freiman and H. Halberstam, On a product of sines, *Acta Arithmetica* **XLIX** (1988), 378-385.

[5] A. O. Gelfond, Sur les nombres qui ont des proprietes additives et multuplicatives donnees, *Acta Arithmetica* **XIII** (1968), 259-265.

[6] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*,Elsevier/North Holland, 1977.

[7] D. I. Newman, On the number of binary digits in a multiple of three, *Proc. AMS* 21 (1969), 719-721.

[8] D. Redmond, *Number Theory: an Introduction*,Marcel Dekker, N.Y., 1996.

[9] V. Shevelev, Estimates of Newman sum over multiples of a fixed integer, *arXiv (math. NT)*, 0804.0144 .

[10] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences (http://www.research.att.com)

Department of Mathematics, Ben-Gurion University of the Negev, Beer-Sheva 84105, Israel. e-mail:shevelev@bgu.ac.il